State of North Dakota

Information Technology Department

Appropriate Usage White Paper

Final Version 1.1
12/24/01

Table of Contents

PURPOSE AND INTENT: 3
EXECUTIVE SUMMARY AND RECOMMENDATIONS: 3
BACKGROUND AND RESEARCH: 4
THE UNIVERSITY OF BRITISH COLUMBIA TASK FORCE 4
THE AMERICAN MANAGEMENT ASSOCIATION SURVEY 4
OTHER STATES 5
South Dakota *5*
Montana *5*
Kansas *5*
Iowa *6*
NORTH DAKOTA AGENCIES 6
Attorney General *6*
Bank of North Dakota *6*
Department of Human Services *6*
Department of Transportation *6*
Information Technology Department *6*
Office of Management and Budget *6*
Secretary of State *7*
Unified Judicial System *7*
MONITOR, FILTER OR NOTHING: 7
DO NOTHING 7
Pros *7*
Cons *7*
FILTERING 7
Pros *7*
Cons *7*
MONITORING & REPORTING 8
Pros *8*
Cons *8*
SUMMARY: 8
APPENDIX A: SUGGESTED APPROPRIATE USE POLICY 9
APPENDIX B: LOCATION OF UNIV. OF BC TASK FORCE REPORT 12
APPENDIX C: SOUTH DAKOTA - COMPUTER-EMAIL-INTERNET USAGE POLICY 13
APPENDIX D: MONTANA 14
APPENDIX E: KANSAS 18
APPENDIX F: ATTORNEY GENERAL'S OFFICE 20
APPENDIX G: BANK OF NORTH DAKOTA 22
APPENDIX H: DEPARTMENT OF HUMAN SERVICES 29
APPENDIX I: DEPARTMENT OF TRANSPORTATION 32
APPENDIX J: INFORMATION TECHNOLOGY DEPARTMENT 34
APPENDIX K: OFFICE OF MANAGEMENT AND BUDGET 36
APPENDIX L: SECRETARY OF STATE 38
APPENDIX M: UNIFIED JUDICIAL SYSTEM 40

Information Technology Department Appropriate Usage White Paper

Purpose and Intent:

This paper will review the need for a statewide Appropriate Use Policy for business communications and give a recommendation on what that policy should be.

This paper will also discuss the concepts of monitoring and filtering of the Internet, list the positives and negatives of each, and give a recommendation on how the state of North Dakota should pursue this issue.

Executive Summary and Recommendations:

Appropriate Use Policy

Research indicates that most policies on the issues of appropriate usage of the Internet and e-mail are issued from the Human Resources (HR) departments. The reasons cited being that most inappropriate usage falls under laws and policies already in existence such as Sexual Harassment (hostile work environment) and Title VII policies (Civil Rights). With that in mind, several areas within the Information Technology Department (ITD) and Central Personnel (CPD) worked together to come up with a draft policy. It is the intention of this policy to be a baseline for agencies to use. Agencies may enact a stricter policy if they wish. This policy is attached as Appendix A. The following is some of the key features recommended:

- Allows users to access the Internet for non-job related purposes provided that it meets the following guidelines:
    - Does not interfere with the performance of the employee's public duties;
    - Is of nominal cost or value;
    - Does not create the appearance of impropriety;
    - Is not for a political or personal commercial purpose;
    - Is reasonable in time, duration, and frequency; and
    - Makes only minimal use of hardware and software resources.
- The user must also follow a list of standards of conduct. Some of the standards are:
    - Must use the Internet in a professional and ethical manner;
    - Must not use electronic communication devices for harassment or other inappropriate behavior regarding race, color, creed, religion sex, ancestry, national origin, age or disability;
    - Must not use electronic communication devices to access, display, archive, store, distribute, edit or record sexually explicit material.
    - Must not create or distribute immoral, obscene, threatening, defrauding or violent text or images or transmit inappropriate or unlawful materials;
- Other standards cover copyright laws, authorized access, illegal activity, pirated software and viruses.

It is strongly recommended that this or a similar policy be instituted statewide. It would help limit the state's liability while providing employees a clear guideline and set expectations of privacy.

Monitoring and Filtering

The state of North Dakota has three choices in regards to monitoring and/or filtering of the Internet.

- Do Nothing:
    - Most cost effective in the short term as there is no further investment in technology.

- Leaves the state most at risk for liability on Sexual Harassment and Title VII suits.

- Filter:
  - Least cost effective both short term and long term.
  - Issues with over filtering and legitimate searches on banned sites (criminal investigation).
  - Issues with censorship.
  - Least risk of liability.
- Monitor & Report:
  - Requires some technology investment.
  - Reporting would give agencies information to apply to their usage policy.
  - Employee notification of this procedure should take care of most inappropriate use.
  - Decreases risk of liability.

It is the consensus of ITD that monitoring and reporting would be the best choice for the state of North Dakota. In a recent test, over a 9-day period, ITD Security found that Adult/Sexually Explicit, Games, and Gambling traffic consumed only about 1.5% of our total Internet traffic. This does, however, equate to over 31,000 connections in 9 days to those areas. The primary thought is to balance the cost factors versus the cost of public trust. If monitoring and reporting does not take care of the issue, the state will still be able to investigate the more costly option of initiating filtering.

Background and Research:

The following are the details of the research performed. This research along with interviews of ITD and CPD personnel were used to form the opinions presented in this paper.

The University of British Columbia Task Force

The University of British Columbia formed a task force to address the issue of appropriate usage of computer equipment owned by the University. The task force issued its report in 1992. While significant changes have occurred during the intervening years, the primary conclusions of the task force are still valid. Those conclusions are as follows:

- Information Technology is just another form of communication. Like the telephone or fax, the rules that cover those tools should be applied to computer technology.
- There are already laws that cover most appropriate use situations, i.e. Sexual Harassment, Civil Rights, etc.

Appendix B contains the Internet location to the full report issued by the task force.

The American Management Association Survey

The American Management Association (AMA) performs an annual survey. They produced a summary of key findings about workplace monitoring and surveillance. The full survey can be found at http://www.amanet.org/research. Some of the key findings are as follows:

- Approximately 62% of the businesses surveyed monitor their Internet connection.
- Approximately 42% of the businesses surveyed store and review E-mail messages
- Approximately 36% of the businesses surveyed store and review computer files.

- Below is a table of why the surveyed businesses monitored and the average importance rating given to that rationale. Importance was rated as 1 being the lowest and 7 being the highest.

	Whole Sample		hose who had Legal Action already occur	
Rationale	Avg. mportance Rating	Pct ating High (6 or7)	Avg. Importance Rating	Pct Rating High (6 or7)
Legal Liability	5.89	68.3%	6.30	81.8%
Security Concerns	5.65	60.0%	5.56	60.6%
Productivity Measurement	5.06	45.5%	5.08	42.4%
Legal Compliance	5.04	50.1%	4.48	60.6%
Performance Review	3.70	45.3%	3.89	25.8%

- Ninety-five percent of companies that actively monitor employees have written policies.
- Seventy-five percent of companies that do not actively monitor employees have written policies.
- Also revealing are the restrictions set on connections to various types of websites. Bear in mind that only 38% of respondent firms use “blocking” software to prevent internet connections to unauthorized or inappropriate sites, so in many companies these restrictions must be enforced by monitoring:

	Whole	**Written Internet Policy**		**Active Monitoring**	
Restricted Websites	**Sample**	**Yes**	**No**	**Yes**	**No**
“Adult” sites with explicit sexual content	76.6%	81.5%	59.6%	80.3%	66.1%
Game sites	26.4%	29.2%,	17.2%	28.8%	20.0%
Entertainment sites	17.7%	19.6%	11.1%	19.4%	13.0%
Sports sites	14.7%	16.4%	9.1%	16.6%	9.6%
Shopping sites	13.1%	15.8%	4.0%	15.6%	6.1%
Other sites	11.5%	12.2%	9.1%	12.8%	7.8%

Other States

Several other state’s policies were also reviewed. Below is a listing and some brief comments on each policy.

South Dakota

South Dakota has a 16-point document that clearly spells out their position on Internet and e-mail usage. In general, state equipment is not to be used for other than state business purposed. The actual policy is attached as Appendix C.

Montana

Montana’s posted policy was a very general overall policy. The three primary items forbidden are as follows:

- "for-profit" activities
- "non-profit" or public, professional or service organization activities that aren't related to an employee's job duties
- for extensive use for private, recreational, or personal activities.

It also covers privacy and copyright material. It then directs the individual agencies to have a “clear policy” on the issue and then provides some guidelines for them. The full policy can be found as Appendix D.

Kansas

Kansas’ statewide policy is that only official state business should be conducted on the Internet. However, it does give agency heads the ability to change that provided all costs are accounted for and the state is reimbursed. The full policy can be found as Appendix E.

Iowa

Iowa has a simple statement in their employee handbook that says:

> Internet service is provided by the state of Iowa to support open communications and exchange of information, as well as to provide the opportunity for collaborative government-related work. The state of Iowa encourages the use of electronic communications by its employees. Like any resources made available to employees of the state, use of the Internet service is a revocable privilege. The use of state-provided Internet service must be for state government-related activities and not for personal business, for-profit activities, commercial advertising, entertainment or other use that interferes with an employee's productivity or reflects poorly on state government. Misuse of the Internet could be grounds for disciplinary action up to and including discharge.

North Dakota Agencies

Some North Dakota agencies already have policies in place. The draft policy found in Appendix A was based upon several of the existing policies. In no case would the draft policy place additional restrictions upon those agencies that already have a policy. Below are the agencies who provided ITD with a copy of their policy and highlights of the policy.

Attorney General

The Attorney General's Office had one of the clearest and most specific policies of those reviewed. It covers Training, Appropriate Use, and Standards of Conduct. Much of the verbiage of the draft statewide policy came from this document. See Appendix F for the AG's complete policy.

Bank of North Dakota

The Bank of North Dakota has a very formalized policy. It is highly structured and very detailed. It also contains a very clear privacy statement. See Appendix G for BND's complete policy.

Department of Human Services

The Department of Human Services expanded the policy to a more general "technology usage". It includes unauthorized software and downloads, virus protection, and laptop usage as well as Internet and e-mail usage. The policy also notes specifically when non-business use would be acceptable and what would not be acceptable at any time. See Appendix H for DHS's complete policy.

Department of Transportation

DOT's policy is very similar in form and format to the Attorney General's policy. It also adds the warning that the Internet is not a secure environment. See Appendix I for the DOT's complete policy.

Information Technology Department

ITD's policy is fairly detailed but relaxed. It addresses putting state owned information in a publicly accessible location. The Internet and e-mail are handled as separate issues. See Appendix J for ITD's complete policy.

Office of Management and Budget

OMB is another well laid out policy. This policy includes the telephone and fax machines in a more general business communications policy. This concept was used to formulate the recommended policy in Appendix A. The policy still has several gray statements such as "inappropriate". This policy also details out record retention requirements. See Appendix K for OMB's complete policy.

Secretary of State

The Secretary of State's policy is very similar to OMB's policy. A key feature of this policy is a separate signoff form (SNF 51554). This concept was also included in our recommended policy. See Appendix L for the Secretary of State's complete policy.

Unified Judicial System

This policy covers general computer usage, software and data usage, as well as Internet and remote access. It also specifically speaks to the agencie's right to install software to "measure and manage Internet and Remote Access usage." This policy also clearly covers issues regarding copyrighted material. See Appendix M for the Unified Judicial System's complete policy.

Monitor, Filter or Nothing:

The state has three choices regarding tracking Internet usage. Below is an examination of the pros and cons of all three options. One note, unless specifically stated, these items do not include Higher Education or K-12.

Do Nothing

Currently ITD logs Internet traffic to a file to be used for investigation purposes. No reports are generated from this information. So, the first option for the state is to choose to do nothing more.

Pros

- This is the most cost effective for the short term as there are no additional expenses incurred
- Privacy issues are minimized, as only IP addresses are stored.
- There are no issues regarding censorship.

Cons

- This choice leaves the state the most liable in regards to Sexual Harassment and Civil Rights violations.
- This choice also has the highest risk of loss of public confidence.
- Individual agencies may choose to implement security on their own. This could lead to multiple packages and rules that could have a significant impact on the network.

Filtering

Next, the state could choose filter the Internet. While this gives the state the most control over what happens on it's network, there are some major concerns that would need to be addressed.

Pros

- This gives the state the most protection for liability in regards to Sexual Harassment and Civil Rights violations.
- This option "removes temptation." Since employees are prevented from getting to inappropriate sites, they can't be tempted to "just check it out."
- ITD could control one type of solution.

Cons

- Most filtering solutions would need to be placed between the firewall and the clients. This adds a failure point to the network. It could also create a bottleneck in the network impacting overall network speed.
- Over blocking could be a concern. This means that an acceptable site may be blocked due to a system misunderstanding. A common example: A site dealing with breast cancer may be blocked because it contains the word breast. This could be mitigated depending upon the solution chosen, but the more manual intervention required leads us to the next point;
- This solution could have a significant impact upon the IT Security section. Sites that the chosen solution could not classify would need to be manually investigated. Certain state personnel require full access (such as law enforcement) that would

require setting up and maintaining specific exemptions for individual PCs. This list could easily grow quite large.

- This solution has the highest issue with censorship. It could also impact morale as a loss of trust could be implied.
- This solution has the highest cost in regards to both short and long term. Hardware and/or software would need to be purchased and maintained. A database would also need to be maintained which could grow quite large depending upon how much the state chooses to filter.

Monitoring & Reporting

The key here is both needs to happen. Guidelines for abuse would need to be developed and employees would need to be notified of the program.

Pros

- This gives the state the some protection for liability in regards to Sexual Harassment and Civil Rights violations.
- This process would occur off-line and so would have a minimal impact on the network.
- This choice would minimize censorship concerns and should have a low impact on morale.
- Once employees are notified of the process, it should take care of most of the inappropriate traffic.

Cons

- The state would still incur additional costs for the hardware and/or software. There still would be database costs, but it would probably be lower than if filtering would be implemented.
- Privacy issues would still be a major concern, but adopting the recommended policy in Appendix A could mitigate this.
- Leaves us more vulnerable to the Open Records Law. Mitigation of this would require some examination of the law, security, and privacy.

Summary:

After reviewing the above research and interviewing CPD and ITD personnel, the following are the author's recommendations:

- In order to mitigate the state's liability under sexual harassment and Title VII laws, each agency needs to implement an enterprise-wide appropriate usage policy setting the minimum standards that individual agencies would follow. An agency would be free to enact stricter regulations. A baseline example provided by ITD can be found in Appendix A.

- The state should move forward in implementing an Internet Monitoring & Reporting Policy. This project would require some additional research into exactly what would be the best specific solution to implement.

- The Senior Advisory Committee and ITD should meet to determine specific reporting procedures and processes. This group should also maintain contact with the next group.

- A group of agency human resource representatives should get together and draft guidelines on the appropriate usage policy and an employee education program.

- Research into privacy and Open Records laws should take place looking specifically at how these reports would fall under Open Records and draft any changes that it is felt need to be recommended.

Appendix A: Suggested Appropriate Use Policy

The State of North Dakota's Appropriate Usage Policy for Electronic Communication Devices

Scope and Purpose:

The state of North Dakota provides Electronic Communication Devices (ECDs) designed to facilitate business communications among state employees and other business contacts. Those devices include telephone, facsimile (fax) machines, all computer software (including e-mail and Internet), and any other type of electronic communication. These devices are state property and are provided to be used for business purposes only.

Full & part-time employees, contractors, consultants, and temporaries are expected to communicate in a professional manner that will reflect positively on them and the state of North Dakota. It is the intent of the state of North Dakota to provide a policy that will ensure that our employees use all ECDs appropriately. It is the intent of this policy to provide a baseline for all North Dakota agencies. Individual agencies may enact a stricter policy.

Use of Electronic Communication Devices:

The Internet (World Wide Web) is a vast global network linking computers at sites around the world and it is a vital source for researching and accessing information, communicating through electronic mail (e-mail), and using on-line services. Employees are encouraged to become familiar with and use the Internet's resources to enhance productivity. The state is responsible for controlling the use of the Internet in a reasonable manner to prevent or detect abuse and avoid legal exposure.

- **Authorized Use:** All employees are authorized to use the Internet for a purpose related to their employment or official positions. However, an employee may use the Internet for a non-governmental purpose provided the use:
    - Does not interfere with the performance of the employee's public duties;
    - Is of nominal cost or value;
    - Does not create the appearance of impropriety;
    - Is not for a political or personal commercial purpose;
    - Is reasonable in time, duration, and frequency; and
    - Makes only minimal use of hardware and software resources.
- **Standards of Conduct:** An employee's use of an ECD is a privilege, not a right. An employee is solely responsible and shall be personally liable, legally, financially, or otherwise, for the employee's use of ECDs outside the scope of the employee's employment. An employee:
    - Must use the Internet in a professional and ethical manner;
    - Must not use electronic communication devices for harassment or other inappropriate behavior regarding race, color, creed, religion sex, ancestry, national origin, age or disability;
    - Must not use electronic communication devices to access, display, archive, store, distribute, edit or record sexually explicit material.
    - Must not create or distribute immoral, obscene, threatening, defrauding or violent text or images or transmit inappropriate or unlawful materials;
    - Must not create, distribute, copy or knowingly use unauthorized copies of copyrighted material or software, store such copies on state of North Dakota computers, or transmit them over the state networks;
    - Must use the Internet only to access files that are publicly available or to which the employee has authorized access;
    - Must not use electronic communication devices for illegal activity;

- Must not use state equipment to knowingly download or distribute pirated software or data;
- Must not knowingly distribute viruses or bypass any detection system in place;

The State of North Dakota's Appropriate Usage Policy for Electronic Communication Devices

- Is responsible for any charges associated with billable Internet services unless appropriate authorization has been obtained prior to accruing the charge;
- Must not execute, open or distribute downloaded Internet information, images, text or public domain software unless it is first checked for a virus; and
- Should be aware that all electronic communications is public information and is subject to disclosure per North Dakota's Open Records Law.

Training:

The Agency will offer adequate training for employees on using ECDs so the employees become more informed, knowledgeable, and productive. The training will teach employees how to use the Internet and e-mail effectively and avoid unlawful use. Training may include, but is not limited to, software, books, on-line training, and off-site and in-house training.

Measuring and Monitoring:

The state of North Dakota reserves the right to install software to measure, manage, and monitor all electronic communication devices, including but not limited to storing, accessing, and reviewing information received or sent through e-mail or over the Internet and logging and analyzing sites accessed and denied. The state reserves the right to block out any Internet sites deemed by the state to be unrelated to the state's responsibilities. The state will cooperate with any legitimate law enforcement investigation.

Non-compliance Measures:

An employee's inappropriate conduct may lead to disciplinary actions up to and including termination of employment.

Acknowledgement:

All current full and part-time employees, and temporary employees are required to sign a Business Communication Acknowledgement Form. New full-, part-time and temporary employees are required to sign this form upon acceptance of employment/contract. All new contracts must have a clause identifying this policy and the contactor's acceptance of the policy.

Electronic Communication Devices Policy
Acknowledgement Form

By signing this form, I acknowledge the following:

I understand that all electronic communication devices, including but not limited to, telephone, facsimile (fax) machines, computers (including e-mail and the Internet) and all information transmitted by, received from, or stored in these systems are the property of the state of North Dakota.

I understand that these systems are not to be used for soliciting outside business ventures, advertising or soliciting for personal enterprises.

I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt or storage of information in this equipment.

I understand that this equipment can be monitored at any time.

I have read and understand my agency's Appropriate Usage Policy for Electronic Communication Devices.

_____

Employee's Name (Please Print)

_____

Employee's Signature Date

☐ *I have been trained on computer security and appropriate usage.*

_____

Employee's Signature Date

Appendix B: Location of Univ. of BC Task Force Report

The full text of the task force's report can be found at http://www.cs.ubc.ca/doc/world/tfauit/cover.

Appendix C: South Dakota - Computer-Email-Internet Usage Policy

1. The state's computer equipment, email system and Internet access facility is limited to use for official state business only, none of which should be used for personal communications, personal gain or advancement of individual views.
2. Computer games and unlicensed software will not be permitted on state computers.
3. Employees may not use the state's Internet facilities to download entertainment software or games, or play games against opponents over the Internet.
4. The state reserves the right to monitor and block access to all inappropriate Internet sites.
5. The state reserves the right to inspect any and all files stored in public or private areas of the state's computers and networks to assure compliance with this policy.
6. Any software or file downloaded via the Internet into the state network or any state computer becomes the property of the state.
7. The use of a computer, email or the Internet for harassment or other inappropriate behavior regarding race, color, creed, religion sex, ancestry, national origin, age or disability is prohibited.
8. Sexually explicit material may not be accessed, displayed, archived, stored, distributed, edited or recorded using state network or computing resources.
9. Use of any state computer or network resource for illegal activity is not permitted and the state will cooperate with any legitimate law enforcement investigation.
10. No employee may use state facilities knowingly to download or distribute pirated software or data.
11. No employee may knowingly distribute viruses or bypass any detection system in place.
12. Employees may download software pertaining to direct business use, not on BIT's standards list, with BIT's approval. Employees must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.
13. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the state may speak/write in the name of the state to any newsgroup or chat room.
14. Employees with Internet access may not upload any software licensed to the state or data owned or licensed by the state without explicit authorization from BIT. Example: the GIS digital orthoquads of South Dakota (data used to produce maps) were purchased and licensed for state use only.
15. The use of news briefing services like Pointcast or any other "pushed" information software is permitted only with BIT's approval.
16. Use of instant messaging services is permitted only with BIT's approval.

Violations of any these provisions may result in discipline up to and including termination.

Appendix D: Montana

Enterprise-wide Policies

Number: ENT-INT-011

Policy: Internet Services

Established for: State of Montana Information Technology Enterprise

BARBARA RANF, Director
Department of Administration

Date: August 2, 2001

Policy - **Requirements**

SCOPE

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to public access computers, and students/employees of the Montana University Systems who are employed by the System and are not full time employees.

INTERNET ACCEPTABLE USE

The State provided Internet, intranet and related services are to be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; and conducting other appropriate State business.

The State provided Internet, intranet and related services are not to be used for: 1) "for-profit" activities, 2) "non-profit" or public, professional or service organization activities that aren't related to an employee's job duties, or 3) for extensive use for private, recreational, or personal activities.

Employees should not have expectations of privacy for Internet use. Agency System Administrators, management, and Department of Administration personnel can monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected.

Employees must follow all other state policies when using the state provided Internet service. See policy ENT-SEC-081 User Responsibilities for additional information regarding the use of state computer resources.

COPYRIGHT LAWS

State employees must honor copyright laws regarding protected commercial software or intellectual property. Duplicating, transmitting, or using software or other electronic property not in compliance with license agreements is considered copyright infringement. State employees are not to make copies of any copyrighted materials without the full legal right to do so. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyrighted material from the Internet, but its use must be strictly

within the agreement as posted by the author or current copyright law. In addition, copyrighted agency/State information used on web sites must be clearly labeled as such.

AGENCY RESPONSIBILITIES RELATED TO THE INTERNET

Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use.

Please see the policy guidelines for assistance in creating your agency policy.

Background - **History on the creation of or changes to this policy**

The ITAC Internet Policy Advisory Task Force worked during 1997 to study the need for policy for state government use of the Internet. The Task Force identified potential areas of risk, researched existing policy and law, and determined whether there was additional need for policy. The Task Force found that educating agencies and employees with a compilation of existing policy, law and guidelines would provide direction to agency and employee Internet users. The results of the Task Force's work are this policy and its guidelines and recommendations to ITAC regarding changes to existing policies.

The ITAC Internet Policy Advisory Task Force was comprised of representatives from the following agencies and organizations:

> The Commissioner of Higher Education, the Public Service Commission, the Department of Agriculture, the Department of Administration's Information Services Division, the Department of Commerce, the Department of Transportation, the Department of Environmental Quality, the Department of Justice, the Office of Public Instruction, the Legislative Branch, the Department of Public Health and Human Services, the State Fund, the State Auditor's Office, the State Library, the Governor's Office, the Department of Fish, Wildlife and Parks, the Department of Labor and Industry and the Department of Revenue

Guidelines - **Recommendations, not requirements**

The Internet has been provided to State employees for the benefit of agencies and their customers. Every State employee has the responsibility to maintain and enhance the State's public image and to use the Internet in a productive manner. To ensure these standards are being met, the following guidelines have been established for assisting agencies in developing their agency business use policies for the Internet, intranet and related services.

> *"Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare."*

Agencies should be in compliance with existing statewide and agency laws, rules and policies. Following are some examples of the existing laws, rules and policies for consideration when creating agency business use policies. Other laws, rules and policies may be applicable.

LAWS AND RULES

- MCA 2-2-121 - Rules of Conduct for Public Officers and Public Employees
- MCA 2-17-322 - Electronic Access Systems
- MCA 45-6-311 - Unlawful Use of a Computer

- ARM 2-21-1105 - Cost/Benefit Analysis Criteria
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 1-0250.00 - Information System Security
- MOM 1-0232.30 - Software Support by Department of Administration
- MOM 1-1103.01 - Use of State Telephone System, Personal Telephone Use

*In addition, agencies should be aware that issues of Federal law and individual rights may also apply.

POLICIES

- SummitNet Acceptable Use
- Aggressive Use of Information Technology to Provide Citizen Access to Information and State Services
- Access of State Computer Systems by Employees, Agents, or Contractors via Asynchronous Comm
- Transmission Privacy
- Computer Virus Detection & Prevention
- User Responsibilities
- Server Maintenance

Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use. Following are items and examples for consideration when creating agency business use policies. Other issues may be applicable.

GUIDELINES

- All State employees shall be provided an opportunity for appropriate training in the use of automated information systems hardware and software used in the performance of their day-to-day responsibilities. Use of technology that meets ethical standards and provides exposure, education or experience should be allowable and encouraged under each agency policy.
- Agency policy should ensure Internet and intranet solutions are cost effective.
- Agencies should appoint and/or maintain an Internet contact person, including an e-mail address on the agency Web site.
- Information confidential under State law should not be transmitted (including e-mail) via the Internet without appropriate security measures taken to safeguard the information.
- Agency pages should contain:
    - Information on how to contact the agency by e-mail, regular mail and telephone
    - A link back to the State home page

- Home pages reflect the image of the State of Montana and your agency; all information should reflect the State and agency standards for quality.
    - It is important for agencies to establish an ongoing process for updating the content, appearance, and usability of all information supplied to the public.
    - Disclaimers don't necessarily protect an agency from liability due to misinformation. If an agency has inaccurate information on their web site and the public relies on it, the agency may be liable.
    - All Internet options, page links, graphic links, and URL links should be verified regularly for accuracy and appropriateness.
    - A procedure and standard should be established for responding to inquiries and comments received through the Internet. Customers should be provided timely and responsive acknowledgments to queries and requests.
    - Agencies should log and regularly analyze Web page access statistics to evaluate server utilization, customer sources and access frequencies for various files.
    - Agency policies should include Web page design standards to ensure access by persons with disabilities. Pages should contain a text-based parallelism. To ensure access, pages can be tested using Cast's Bobby at http://www.cast.org/bobby. More information on creating accessible web pages can be found at http://www.trace.wisc.edu.
- Agency policies should require utilization of any Electronic Data Interchange (EDI) standards that have been adopted by government or industry to ensure compatibility and interoperability with other State agencies and to the extent practicable with non-state information systems.

All entities that use the state's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

References - **Laws, rules, standard operating procedures and applicable policies**

2-17-501, MCA; 2-17-503, MCA; 2-15-112, MCA; ARM 2.13.101 - 2.13.107; SummitNet Acceptable Use Policy

Return to IT Policies Page

Return to ISD Home Page

Appendix E: Kansas

POLICY #1200 REVISION #0

KANSAS INFORMATION RESOURCES COUNCIL

INFORMATION TECHNOLOGY POLICY #1200 REVISION #0

1.0 TITLE: Acceptable use of the Internet

1.1 EFFECTIVE DATE: December 1, 1996

1.2 TYPE OF ACTION: New

2.0 PURPOSE: To establish a common, uniform use policy for all state agencies regarding use of the Internet by employees.

3.0 ORGANIZATIONS AFFECTED: All divisions, departments and agencies of the state.

4.0 REFERENCES:

4.2 K.S.A. 75-4741 authorizes the KIRC to: provide direction and coordination for the application of the state's information resources.

5.0 DEFINITIONS: The following definitions are applied throughout this policy and procedure memorandum.

5.1 **Official State Internet Use** is the access to or distribution of information via the Internet by state officers or employees which is in direct support of Official State Business. "Official State Business" is defined in K.A.R. 1-17-1 as "The pursuit of a goal, obligation, function, or duty imposed upon or performed by a state officer or employee required by employment with this state."

5.2 **Other Appropriate Use.** By authorizing the payments for access to KAN-WIN and/or the Internet Service Provider the head of a State Agency has the implicit authority and responsibility to determine when and under what circumstances the officers and employees of that agency can use the Internet for activity other than described in 5.1.This will constitute other appropriate use.

6.0 POLICY: In order to establish a common, uniform policy for all state agencies regarding use of the Internet, the following procedures are established.

6.1 Officers and employees of the state shall not use the Internet for other than official business unless the heads of their agencies have established written policies regarding other appropriate use of the Internet.

6.2 The head of any state agency may establish a policy in writing to allow officers and employees of that agency to use the Internet, provided that any costs associated are properly reimbursed, and that the use policy prohibits illegal and unethical practices.

6.3 Each agency that has established policies, or that establishes new policies and procedures for use of the Internet shall maintain on file a copy of those written policies and procedures. The written policy must contain well-defined procedures to account for Internet activity and to recover the costs for this activity if appropriate.

6.4 Any officer or employee of the state who violates the provisions of their respective agency's policies and procedures, or the procedures of this policy and procedure memorandum regarding Internet activity, shall be subject to disciplinary action, including, but not limited to demotion, suspension, and termination. In every case, however, the offending officer or employee shall be required to reimburse the state for the total value of any Internet fees incurred in violation of this policy and procedure memorandum and of any state agency=s established policies and procedures.

7.0 PROCEDURES:

7.1 Agencies must publish and distribute the Internet policy to all employees of the respective agency by March 1, 1997.

8.0 RESPONSIBILITIES:

8.1 Heads of divisions, departments, agencies, boards and commissions are responsible to establish procedures for their organizations to comply with the requirements of this policy.

8.2 The Chief Information Architect is responsible for the maintenance of this policy.

9.0 CANCELLATION: None.

10.0 CONTACT PERSON: Fred Boesch, Chief Information Architect (or Designee).

Appendix F: Attorney General's Office

Office of Attorney General Internet and e-mail policies

4-18.5 Use of the Internet and internal e-mail. The Internet (World Wide Web) is a vast, global network linking computers at sites around the world and it is a vital source for researching and accessing information, communicating through electronic mail (e-mail), and using on-line services. Employees are encouraged to become familiar with and use the Internet's resources to enhance productivity. The office is responsible for controlling the use of the Internet in a reasonable manner to prevent or detect abuse and avoid legal exposure.

1) Authorized Use. All employees of the Office of Attorney General are authorized to use the Internet for a purpose related to their employment or official positions. However, an employee may use the Internet for a non-governmental purpose provided the use:

   a) Does not interfere with the performance of the employee's public duties;

   b) Is of nominal cost of value;

   c) Does not create the appearance of impropriety;

   d) Is not for a political or personal commercial purpose;

   e) Is reasonable in time, duration, and frequency; and

   f) Makes only minimal use of hardware and software resources.

2) Training. The office of Attorney General will offer adequate training for employees on using the Internet and internal e-mail so the employees become more informed, knowledgeable, and productive. The training will teach employees how to use the Internet and internal e-mail effectively and avoid unlawful use. Training may include software, books, and off-site and in-house training.

3) Standards of Conduct. An employee's use of the Internet is a privilege, not a right. An employee is solely responsible and shall be personally liable, legally, financially, or otherwise for the employee's use of the Internet outside the scope of the employee's employment. An employee's use within the scope of employment shall be treated as other activities undertaken by the employee within the scope of employment. An employee's inappropriate conduct may lead to disciplinary action, including restricting the employee's access and use of the Internet or other appropriate action. An employee:

   a) Must use the internet in a professional and ethical manner;

   b) May not create or distribute immoral, obscene, threatening, defrauding, or violent text or images or transmit inappropriate or unlawful materials through the Internet;

   c) Nay not enter or send obscene or offensive material into or through the Internet;

   d) May not create, distribute, or knowingly use unauthorized copies of copyrighted material on the Internet;

   e) Must use the Internet only to access files that are publicly available or to which the employee has authorized access;

   f) Must refrain from overloading the network with excessive date or wasting computer time, connect time, disc space, printer paper, or other resources;

   g) Is responsible for any charges associated with billable Internet services unless appropriate authorization has been obtained prior to accruing the charge;

h) May not use illegal copies of copyrighted software, store such copies on Office of Attorney General computers, or transmit them over the state networks;

i) May not execute or distribute downloaded Internet information, images, text, or public domain software unless it is first checked for a virus; and

j) May be aware that all E-mail communications are public information and are subject to disclosure to management, other state agencies, or the public unless restricted by law from disclosure. E-mail must e composed as formal professional type of Office of Attorney General communication. Slang, misspellings, abbreviations, and messages that may be interpreted as sexual harassment must be avoided. An employee may not use E-mail:

   i) To harass, intimidate, or annoy another person;

   ii) To send foul, inappropriate, romantic, or offensive messages; or

   iii) To solicit outside business ventures or for political or religious causes.

4) Internal e-mail. E-mail between employees of the Office of Attorney General or within the state system, but not sent through the Internet, is subject to the same restrictions as use of the Internet except as authorized in Section 21-3 for solicitations for contributions or time or money.

The Office of Attorney General may install software to measure, manage, and monitor Internet and internal e-mail usage by employees, including accessing and reviewing information received or sent through internal e-mail or over the Internet and logging and analyzing sites accessed and denied. The office may block out any Internet sites deemed by the office to be unrelated to the office's responsibilities.

Revised April 15, 1998

Appendix G: Bank of North Dakota

BND

Email Security

Policy Type: *Network Security*	
Department: *Information Technology Services*	
Executive Approval: *06/20/2001*	**Creation Date:** *5 / 01 / 2001*
Creator Name: *Phyllis Lasher*	**Creator Title:** *IT Manager*
Date Last Revised: ___/___/_____	**Reviser Name:** _____

Statement of Fact

This applies to all employees, contractors, consultants, temporaries, and all other users of the Bank of North Dakota network. The guidelines of this policy also apply to those users affiliated with third parties who access this computer network.

All information traveling over the Bank of North Dakota computer network that has not been specifically identified as the property of other parties will be treated as though it is a Bank of North Dakota asset. It is the policy of Bank of North Dakota to prohibit unauthorized access, disclosure, duplication, modification, loss, diversion, destruction, misuse, or theft of this information.

In addition, it is the policy of the Bank of North Dakota to protect information belonging to third parties that has been entrusted to Bank of North Dakota in confidence as well as in accordance with applicable contracts and industry standards.

Section One: Purpose

The purpose of this policy is to establish management direction, procedures and specific instructions on the ways to secure electronic mail (email) resident on personal computers and servers at the Bank of North Dakota.

All policies within apply to Bank of North Dakota employees and contractors and cover email located on all Bank of North Dakota personal computers and servers if these systems are under the jurisdiction and/or ownership of the Bank. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to internal networks.

The Bank of North Dakota encourages the business use of electronic communications such as voice mail, email, and fax as productivity enhancement tools. Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the exclusive property of the Bank of North Dakota, and are not the property of user of the electronic communications services.

Section Two: Privacy

Staff using Bank of North Dakota information systems to send or receive electronic mail should realize that their communications are not automatically protected from viewing by third parties. Bank of North Dakota cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Unless encryption is used, staff should not send private or confidential information through emails unless management approved methods of encryption are applied.

The Bank of North Dakota is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, the Bank of North Dakota is also responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in the interception or disclosure of electronic communications.

It is the policy of the Bank of North Dakota to not regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Bank of North Dakota might from time to time examine the content of electronic communications.

At any time without prior notice, Bank of North Dakota management reserves the right to examine e-mail, personal file directories and other information stored on Bank of North Dakota computers. It may be necessary for Information Technology staff to review the content of an individual employee's communications during the course of problem resolution. Information Technology staff may not review the content of an individual employee's communications out of personal curiosity or at the request of individuals who have not gone through the proper approval channels (Information Technology Manager, President, etc.).

Section Three: Authorized Usage

Bank of North Dakota computing resources and electronic communications systems generally must be used only for business activities. Users are forbidden from using Bank of North Dakota electronic communications systems for charitable endeavors, private business activities, or entertainment purposes unless expressly approved by the Bank of North Dakota president or senior management. Employees are reminded that the use of Bank of North Dakota resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. These facilities should provide the ability to separate the activities of different users. Each employee utilizing the electronic mail system should be given a unique email username and access capabilities appropriate for their job requirements. With the exception of emergencies and regular system maintenance notices, broadcast facilities should not be used unless permission has been obtained.

Employees are reminded that Bank of North Dakota electronic communications system is not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. If encryption technologies are needed, please inquire with the Information Technology Manager.

Section Four: Responsibilities

As defined below, the Bank or North Dakota network administrators and security officers responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.

Users of the Bank of North Dakota electronic mail system must:

1. Know and apply the appropriate Bank of North Dakota policies and practices pertaining to Email security.
2. Not permit any unauthorized individual to access their email account on the Bank of North Dakota network.
3. Not use Bank of North Dakota email system for any purposes other than those authorized by the company.
4. Report to the Information Technology Manager or Information Technology staff any incident that appears to compromise the security of Bank of North Dakota Resources. These include strange messages, potential viruses, and unexplained occurrences that may indicate messages have been compromised.
5. Obtain supervisor authorization before attaching any data files to or from Bank of North Dakota multi-user information systems if this activity is outside the scope of normal business activities.

Section Five: Reporting Security Problems

If users receive a strange email or for some reason feel that one of their electronic communications have been intercepted or otherwise compromised, the Information Technology Manager must be notified immediately. Messages that are suspicious include any email that contains an attachment with the extension .vbs or .cgi, which can signal a potentially serious virus threat. Users should not attempt to open or save these attachments but instead notify the Information Technology Manager so appropriate steps can be taken to minimize virus damage.

If any unauthorized use of the Bank's information systems has taken place, or is suspected of taking place, the Information Technology Manager must likewise be notified immediately. Unauthorized usage includes the sending or sharing of information that could be considered threatening, offensive or harassing. Using the Bank of North Dakota mail system for any type of solicitation is also a direct violation of the usage policy. Employees caught using the email system in one or more of the inappropriate manners outlined will receive disciplinary action up to or including termination.

Contact Point

Questions about this policy may be directed to the Information Technology Manager

Disciplinary Process

Violation of the terms of this or any other security policy may subject employees or contractors to disciplinary procedures up to and including termination.

End-User Computing

Policy Type: *User Security & Guidelines*

Department: *Information Technology Services*

Executive Approval: *06/20/2001* **Creation Date:** *6 / 15 / 2001*

Creator Name: *Phyllis Lasher* **Creator Title:** *IT Manager*

Date Last Revised: ___/___/_____ **Reviser Name:** _____

Section Four: Responsibilities

Bank or North Dakota employees and third parties who use the bank's computer network are responsible for following the practices and policies outlined in the bullet points below.

a) Users must follow email security policies and standards to help prevent unauthorized material from being transmitted across the Internet in a manner that is not secure. They must also exercise caution with regard to email attachments to help prevent virus infestations, hacker intrusions, and similar events.

b) The Internet must only be used in a way that is responsible, and does not compromise network security or open the bank up to attack by hackers or viruses. Inappropriate postings and bank representations on the Internet are not allowed. This includes, but is not limited to claiming to be an official spokesperson for the bank, posting opinions that are implied to be those of the bank, or otherwise falsely indicating that comments made are in any way representative of the Bank of North Dakota, its policies or opinions.

c) Each employee is assigned a unique user ID that they use in conjunction with a password to access network resources. All passwords must meet the Network Authentication guidelines and may never be shared with another employee or third party. Access to network resources should also be protected by logging out of or locking workstations when they are left unattended for more than ten minutes.

d) Access to network resources such as programs, printers and data files is determined on an individual basis. Some users may have access to resources that others do not. If a user feels they need additional access beyond what they currently have, they must submit their request to their manager. The manager will in turn discuss legitimate needs with the Information Technology Manager before a decision is made. Attempts to access unauthorized resources are logged and reviewed on a daily basis by the Bank of North Dakota security officer.

Supplementary information relating to each of the user practices outlined above can be found in detail and separated individually within this policy book. Sections relating to the guidelines above include: Network Authentication, Email Security, End-User Internet Security and others.

End-User

Internet Security

Policy Type: *Network Security*	
Department: *Information Technology Services*	
Executive Approval: 06/20/2001	**Creation Date:** *4 / 25 / 2001*
Creator Name: *Phyllis Lasher*	**Creator Title:** *IT Manager*
Date Last Revised: ___/___/_____	**Reviser Name:** _____

Section Two: Privacy

Staff using Bank of North Dakota information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private or confidential.

At any time without prior notice, Bank of North Dakota management reserves the right to examine e-mail, personal file directories and other information stored on Bank of North Dakota computers. Investigations into Internet usage may include the review of Browser History information or the use of an approved method of tracking visited sites. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Bank of North Dakota information systems.

Section Three: Appropriate Usage

Bank of North Dakota management encourages staff to explore and utilize the Internet as a resource for information. Using the Internet for personal purposes on company time is not considered acceptable usage. Furthermore, games, news groups, and other non-business activities must be performed on personal, not company time and resources as outlined in the End-User Computing Policy.

The Bank of North Dakota reserves the right to restrict the download capabilities of users who have not obtained written permission from the Information Technology Manager. Users who have not acquired permission to download files and proceed to do so will be subject to punishment. Installation of new software by non-Information Technology specialists is strictly prohibited to ensure a safe and virus-free network environment.

Without proper precautions it is relatively easy to fool another user on the Internet. Employees should be aware that the Internet is home to malicious sites and various virus threats that can compromise the security of the Bank of North Dakota network or result in the corruption or loss of critical data.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. It is assumable that a significant amount of Internet information can

be considered either outdated or inaccurate. Contacts made over the Internet should not be trusted with Bank of North Dakota information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal Bank of North Dakota information to a third party.

In accordance with the confidentiality agreements signed by all staff members, Bank of North Dakota software, documentation, and all other types of internal information must not be sold or otherwise transferred to a third party for unless expressly authorized by management. Exchanges of software or data with a third party may not proceed unless a written agreement, detailing the terms of the exchange and the ways in which the software or data is to be handled and protected, has first been signed.

Section Four: Information Protection

Wiretapping and message interception are security threats frequently encountered on the Internet. Accordingly, Bank of North Dakota secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Unless it has been released for public usage, source code must always be encrypted before being sent over the Internet.

Credit card numbers, telephone numbers, network passwords, and other information that can be used to gain access to goods, services or sensitive data must not be sent over the Internet in readable form. An approved method of encryption such as the PGP encryption algorithm, or another algorithm approved by the Information Technology Manager must be used to protect this data before it traverses the Internet.

Bank of North Dakota materials (software, internal memos, etc.) must not be placed on easily accessible machines connected to the internal network or the Internet. Users are prohibited from being involved in any way with the storage or exchange of any of the prohibited materials including: pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material. Any user violating this policy by accessing these or other restricted materials will be reprimanded accordingly.

All publicly writable (or common) directories found on any Bank of North Dakota Internet-connected computers will be reviewed and cleared periodically to ensure no files or programs reside in these directories that should not be there. This process is necessary to prevent the anonymous exchange of information in ways that are not consistent with the Bank of North Dakota's business practices.

Section Five: Public Representations

No external representations can be made on behalf of the company unless they are cleared first with senior management or the president. Additionally, to avoid libel problems, whenever any affiliation with the Bank of North Dakota is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Whenever staff members provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and do not necessarily reflect those of the Bank of North Dakota. These communications must be in strict compliance with the guidelines set by management.

Staff must not publicly disclose internal Bank of North Dakota information via the Internet that may adversely affect the Bank's customer relations or public image unless the approval of senior management or the president has first been obtained. Such information includes but is not limited to: business prospects, unit costing, and RFP information. Responses to specific customer e-mail messages are exempted from this policy, but are subject to the restrictions and guidelines set in the Email Usage Policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If staff members do not exercise proper discretion, they may let competitors know that certain internal projects are underway. If a user is working on an unannounced product, research and development project, or related confidential matter, all postings associated with those activities must be cleared with that division's manager and the president prior to being placed in a public spot on the Internet.

Section Seven: Responsibilities

As defined below, the Bank or North Dakota network administrators and security officers responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

Users of the Bank of North Dakota Internet connections must:

1. Know and apply the appropriate Bank of North Dakota policies and practices pertaining to Internet security.
2. Not permit any unauthorized individual to obtain access to Bank of North Dakota Internet connections.
3. Not use Bank of North Dakota Internet resources (software, hardware or data) for any purposes other than those authorized by the company.
4. Report to the Information Technology Manager or Information Technology staff any incident that appears to compromise the security of Bank of North Dakota Resources. These include missing data, virus infestations, unexplained transactions or passwords that are suspected of no longer being secure.
5. Obtain supervisor authorization for any uploading or downloading of information to or from Bank of North Dakota multi-user information systems if this activity is outside the scope of normal business activities.

Appendix H: Department of Human Services

HUMAN RESOURCE POLICIES AND PROCEDURES
INFORMATION TECHNOLOGY USAGE

North Dakota Department	Division 05	Service 319
of Human Services Manual	Program 301	Chapter 01

SERVICE CHAPTER 319-01

01. Information Technology Usage

01-01. DHS Policy Statement (Revised 7/00 ML #2578)

The following is the North Dakota Department of Human Services' policy regarding the use of information technology. DHS employees may use information systems and technology for government business use. Information technology should not be used to solicit or proselytize others for commercial ventures, religious or political causes, outside organizations, personal use, or other non-job-related solicitations. Misuse of information technology will result in disciplinary action up to and including dismissal.

Limited personal or informal use of Internet access and e-mail is permissible only within reasonable limits with supervisory approval. Please refer to Sections 01-09, 01-11, and 01-13 for additional information.

01-03. Authorized Software/Hardware (Revised 5/97 ML #2396)

Only software that has been licensed by the Department of Human Services or that has been authorized to conduct business is allowed on DHS personal computers and servers. All software purchased and installed must be preauthorized through the Department's Information Management Division (DHS-IMD), unless it meets the standards as established through the Information Management Services Advisory Steering Committee. DHS-IMD maintains the list of approved software standards. Hardware purchases must also follow the approved hardware list, as maintained by DHS-IMD. Employees can request to have software, including shareware, added to the approved list through IMD.

Unauthorized downloading of software is prohibited. All software downloads will be done through authorization of IMD or designee.

The Department of Human Services may audit personal computers (PCs) and servers, and all unauthorized or unlicensed software will be removed. Personal licensed software is not allowed on Department PCs or servers. Employees must adhere to all software and information copyright laws.

01-05. Virus Protection (Revised 7/97 ML #2422)

Computer viruses can cause potential major problems to hardware and software, and can come from nearly any source (Internet, passing of files, etc.) It is essential that all employees be proactive in checking diskettes and their hard drive for viruses. Therefore, DHS-IMD recommends that all files on the hard drive be checked for viruses on a daily basis, and that all diskettes be checked prior to usage. Virus protection software is available for purchase.

To prevent computer viruses from being transmitted through the system, unauthorized downloading of software and shareware from the Internet and other sources is prohibited.

Creating or spreading a computer virus or intentionally causing damage to any Department PC or server is a serious violation to the Department and may be cause for discipline, up to and including dismissal.

01-07. Use of Laptops, Notebooks, Etc. (Revised 5/97 ML #2396)

The use of mobile computers (laptops, notebooks, portable printers, etc.) is supported and encouraged for business use related to the Department of Human Services. Shared mobile computers are available throughout the Department, and may be checked out by employees for specific work-related activities. Written acknowledgment of purpose and duration of checkout will be recorded and signed by the employee who is requesting the equipment. Each unit is responsible for maintaining checkout procedures. Failure to return the mobile equipment in the specified duration may result in disciplinary action. Only Department licensed software is permitted on Department mobile computers.

DHS-IMD strongly encourages sharing mobile equipment that is not part of an employee's full-time daily computing setup.

01-09. E-Mail and Internet General Statement of Policy (Revised 7/97 ML #2422)

The Department of Human Services' e-mail and Internet system is intended to be used for business purposes only; use for informal or personal purposes is permissible only within reasonable limits after business hours with supervisory approval. All e-mail/Internet records are considered Company records and should be transmitted only to individuals who have a business need to receive them. Additionally, as Company records, e-mail/Internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other process. Consequently, employees should always ensure that the business information contained in e-mail/Internet messages is accurate, appropriate and lawful. E-mail/Internet messages by employees may not necessarily reflect the views of the Department of Human Services or it's management. Abuse of the e-mail or Internet systems, through excessive personal use, or use in violation of the law or the Department of Human Services' policies, will result in disciplinary action, up to and including dismissal.

01-11. E-Mail Abuse Intolerance and Other Inappropriate Uses of Computers (Revised 7/97 ML #2422)

The Department of Human Services is adopting and will enforce the following no-nonsense e-mail and document policy. DHS employees will use e-mail for business use. Use for informal or personal purposes is permissible only within reasonable limits after business hours, with supervisory approval.

All electronic communications can be accessed and disclosed to management, attorneys working both for and against the Department, and other government agencies. Please note that electronic information is accessible and could be used for purposes not sanctioned by or under the control of management.

Even deleted messages and documents may be stored in the system for an indefinite duration. The act of deleting a message and document may not totally obliterate it. Because electronic information may continue to exist even after the senders wish to destroy it or wish they had never written it, the same care must be taken in choosing words for electronic information as is taken in more formal types of Department communications. Compose electronic information and messages with the idea in mind that they may someday be used as evidence in court. Courtesy and professionalism should replace slang, intentional misspellings, abbreviations, and over-familiarity.

The Department strictly forbids all electronic message and documents that are discriminatory, defamatory, insulting, romantic, pornographic, or breaches of confidentiality or violation of copyright. Electronic information intended to be humorous or clever can backfire and be taken as sarcastic and annoying. Be especially careful to avoid messages and documents that may be interpreted as sexual harassment.

The Department reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received, or sent over the electronic mail system for any purpose.

01-13. Internet Usage (Revised 5/97 ML #2396)

Internet access is available to Department employees for conducting official business, such as researching business issues, accessing business-related data, information and training. Only business-related work may be conducted on the Internet during the workday.

Employees may use the Internet access after working hours with supervisory approval. Supervisors must monitor how the Internet is used.

Use of the Internet must not disrupt the operation of the Department network or networks of other users. To prevent computer viruses from being transmitted through the system, unauthorized downloading of software from the Internet is prohibited. All software downloads will be done through authorization of IMD.

Misuse of the Department's Internet access during or after work hours is strictly prohibited. All electronic messages and documents that are discriminatory, defamatory, insulting, romantic, pornographic, or breaches of confidentiality or violation of copyright are prohibited. Misuse of the Internet will result in disciplinary action up to and including dismissal.

Appendix I: Department of Transportation

Department of Transportation Internet and e-mail policies

Original Date: 2/16/2001

Revised Date: 2/22/2001

Review By Date: 2/22/2002

POLICY: Authorized Use of Internet. All NDDOT employees who have personal computers are authorized to use the Internet for a purpose related to their employment or official position.

PROCEDURES: The Internet (World Wide Web) is a network linking computers at sites around the world and is a vital source for researching and accessing information, communicating through electronic mail (E-mail), and using on-line services.

1) Authorized use
   An employee may use the Internet for a non-government purpose if the use:
   a) Does not interfere with the performance of the employee's public duties;
   b) Is of nominal cost of value;
   c) Does not create the appearance of impropriety;
   d) Is not personal commercial purpose;
   e) Is reasonable in time, duration, and frequency; and
   f) Makes only minimal use of hardware and software resources.

2) Unacceptable use
   a) Any use that interferes with NDDOT operations or the NDDOT mission statement
   b) Any use that interferes with or disrupts other users, services or equipment
   c) Transmitting any threatening, obscene, sexually-explicit, discriminatory, or harassing materials
   d) Deliberately spreading computer viruses, worms, or trap-door program codes
   e) Gaining unauthorized entry to other information or communication devices or resources
   f) Distributing unsolicited advertising, chain letters, or other blind broadcasting of messages to lists or individuals
   g) Downloading files without specific authorization
   h) Any use that is illegal or violates existing NDDOT policies
   i) Playing computer games or downloading entertainment software

3) Responsibility
   The division, district, and region directors are responsible for controlling the use of the Internet in their assigned areas in a reasonable manner to prevent or detect abuse and avoid legal exposure.

4) Standards of Conduct.
   An employee's use of the Internet is a privilege, not a right. An employee is solely responsible and shall be personally liable, legally, financially, or otherwise for using the Internet outside the scope of his or her job duties. An employee's use within the scope of employment shall be treated as other activities undertaken by the employee within the scope of employment. An employee's inappropriate conduct may lead to disciplinary action, including restricting the employee's access and use of the Internet or other appropriate action. An employee:

   a) Must use the Internet in a professional and ethical manner.
   b) May not create, distribute or knowingly access immoral, obscene, threatening, defrauding, sexually explicit or violent text or images.
   c) May not enter or send obscene, discriminatory or otherwise offensive material through the Internet.
   d) May not create, distribute, or knowingly use unauthorized copies of copyrighted material on the Internet.
   e) Must use the Internet only to access files that are publicly available or to which the employee has authorized access.

f) Must refrain from overloading the network with excessive date or wasting computer time, connect time, disc space, printer paper, or other resources.
g) Is responsible for any charges associated with billable Internet services unless appropriate authorization has been obtained prior to accruing the charge.
h) Should be aware that all e-mail communications are subject to disclosure and that e-mail must not be used:
    1) To harass, intimidate, or annoy another person;
    2) To send foul, inappropriate, or offensive messages.
    3) To solicit outside business ventures.
    4) To send messages that may be interpreted as sexual harassment.
i) No person may intercept confidential communications except as provided by law.

5) The Internet is not a secure environment
Electronic communication must never be considered to be either private or secure. Messages may be sent to incorrect addresses or be forwarded to unappreciative audiences. All existing security polices and procedures must be followed. The Internet is an open environment, so the following precautions must be taken:
    a) All users must be aware of, understand, and comply with existing security measures as outlined in the Computer Security and Disaster Prevention and Recovery Policy Manual.
    b) All users will be held responsible for actions issued from their accounts. Account sharing and password sharing are strongly discouraged.
    c) All users have a responsibility to report security holes and breaches promptly.
    d) All users have a responsibility to use available mechanisms and procedures for protecting their own data.
    e) All electronic data originating outside NDDOT must be downloaded to a floppy (not hard drive) and virus-scanned before use. This includes both FTP data and data received while Internet browsing.

    Internet traffic and use may be monitored and logged. This includes internal and external traffic. No prior notification will be issued.

6) The agency director, division director, region engineer, and district engineer or their designees are the final authority on revoking Internet access for an individual. A single documented unacceptable use may be grounds for revocation. The agency director, division director, region engineer, and district engineer, at their discretion may direct an internal audit of any division, district, or individual without notifying that individual, division or district.

Appendix J: Information Technology Department

INFORMATION TECHNOLOGY DEPARTMENT

POLICY T006-98 EFFECTIVE: SEPTEMBER 1, 1998
UPDATED: MAY 13, 1999

INTERNET USAGE POLICY

PURPOSE:

As part of this organization's commitment to the utilization of new technologies, many of our employees have access to the Internet. It is the intent of the Information Technology Department (ITD) to develop an Internet usage policy that will ensure our employees will use the Internet appropriately and protect ourselves from being victimized by the threat of viruses or hacking into our server.

1. It is ITD's policy to limit Internet access to official business. Employees are permitted to access the Internet for personal business, off-duty, in strict compliance with the other terms of this policy. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited.

2. Employees using ITD's Internet service are acting as representatives of the ITD. As such, public scrutiny and/or disclosure of an employee's Internet usage must not damage the reputation of ITD. Users are expressly prohibited from accessing sites that carry offensive material. Offensive material includes, but is not limited to, pornography and hate literature.

3. Internet Relay Chat channels or other Internet forums such as newsgroups may only be used to conduct work related business or to exchange technical or analytical information. Users who wish to express personal opinions must use a private Internet Service provider.

4. Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect a virus and, if necessary, to prevent its spread.

5. Employees shall not place any State of North Dakota material on any publicly accessible Internet computer without prior permission.

6. The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Employees must exercise caution and care when transferring such material in any form.

7. Alternate Internet Service Provider connections to ITD's internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

8. ITD reserves the right to inspect an employee's computer system for violations of the Internet Usage Policy. Any violation of this policy will subject the employee to disciplinary action, possibly including termination.

INFORMATION TECHNOLOGY DEPARTMENT

POLICY T002-95 EFFECTIVE: MAY 1, 1995
UPDATED: MAY 13, 1999

ELECTRONIC MAIL POLICY

PURPOSE:

The Information Technology Department (ITD) provides an e-mail system designed to facilitate business communication among state employees and other business contacts. It is the intent of ITD to develop an electronic mail policy which will ensure our employees will use the electronic mail system appropriately.

1. Foul, inappropriate, or offensive messages are prohibited.

2. Use of e-mail networks to solicit outside business ventures or political or religious causes is prohibited. Occasional personal e-mail correspondence that complies with the other terms of this policy is allowed, however, it should not detract from work-related activities.

3. Employees will not use unauthorized codes or passwords to gain access to other employees' files.

4. E-Mail messages are capable of being forwarded without the express permission of the original author. Accordingly, due caution should be exercised when sending e-mail messages.

5. E-Mail communications are public documents and may be subject to public review, unless the record is exempt by law from disclosure.

6. ITD reserves the right to monitor e-mail should policy abuse be suspected. Any violation of the Electronic Mail Policy will subject the employee to disciplinary action, possibly including termination.

7. All users of the e-mail system must determine if an e-mail message is considered an official record based on the following criteria:
   a) Made or received under State law or in the conduct of official agency business. For example, a message containing information about the installation of a new telephone system in another state agency.
   b) Preserves evidence of the agency's organization, functions, or other activities. For example, a message relating proposed changes to the organizational structure of Information Technology Department.
   c) Contains information of value relating to agency programs, policies, decisions, and essential transactions. For example, a message containing information to update the Work Schedule Policy.

8. If the e-mail message is identified as an official record, it must be addressed on a records retention schedule. Contact ITD Records Management to update your records retention schedule.

Appendix K: Office of Management and Budget

CHAPTER 12
BUSINESS COMMUNICATIONS POLICY

Section 1. Electronic Communications

1.1 Introduction and Purpose

The Office of Management and Budget (OMB) provides communication systems designed to facilitate business communication among state employees and other business contacts. Those systems include telephone, facsimile (fax) machines, all computer software and any other type of electronic communication. It is the intent of OMB to provide a policy which will ensure that our employees use all communication systems appropriately.

1.2 Prohibited Usage

Foul, inappropriate, or offensive messages are prohibited.

Use of communication systems to solicit outside business ventures or political or religious causes is prohibited.

Advertising or soliciting for personal enterprises and “chain letters” are prohibited.

Employees will not use security features such as codes or passwords without the express knowledge and prior approval of their division director. Employees will not use unauthorized codes or passwords to gain access to other employees’ data.

E-mail messages are capable of being forwarded without the express permission of the original author. Accordingly, due caution should be exercised when sending e-mail messages. No employee may forward any portion of a received message, which has been altered, without authorization from the author. No employee may send e-mail under another employees’ name without authorization.

To avoid introduction of viruses into your computer, exercise caution prior to opening attachments from someone you don’t know. Unsolicited attachments that cannot be verified by the sender should be deleted.

1.3 Accessibility of Records

E-mail communications are public documents and may be subject to public review, unless the record is exempt by law from disclosure.

OMB reserves the right to monitor e-mail to ensure proper use of the system and to protect the interests of the agency. Any violation of the Business Communications Policy will subject the employee to disciplinary action, possibly including termination.

All agency electronic mail is an official public record and is subject to public record regulations with respect to inspection, disclosure, scheduled retention and disposition.

E-mail records must be incorporated into a records retention schedule when they meet the following criteria:

- The message is made or received under state law or in the conduct of official agency business.
- The message preserves evidence of the agency’s organization, functions, or other activities.
- The message contains information of value relating to agency programs, policies, decisions, and essential transactions.

1.4 Policy Exceptions

Divisions of the Office of Management and Budget may adopt more restrictive policies at their own discretion

Occasional personal correspondence that complies with the other terms of this policy is allowed, however, it should not detract from work related activities.

Section 2. Internet Usage

2.1 Introduction and Purpose

It is the intent of the Office of Management and Budget (OMB) to develop an Internet Usage Policy which will ensure that our employees use the Internet appropriately and thereby protect the agency from being victimized by the threat of viruses or hacking into the server.

2.2 Internet Use By Employees

Internet access is limited to official business. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited.

Employees using the Internet are acting as representatives of OMB. As such, public scrutiny and/or disclosure of an employee's Internet usage must not damage the reputation of OMB. Users are expressly prohibited from accessing sites which carry offensive material. Offensive material includes, but is not limited to, pornography and hate literature.

Internet Relay Chat channels or other Internet forums such as newsgroups may only be used to conduct work related business or to exchange technical or analytical information. Users who wish to express personal opinions must use a private Internet service provider.

Employees may not place any State of North Dakota material on any publicly accessible Internet computer without prior permission.

Alternate Internet service provider connections to OMB's internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

Files which are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect a virus and, if necessary, to prevent its spread.

2.3 Accessibility of Records

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Employees must exercise caution and care when transferring such material in any form.

OMB reserves the right to inspect an employee's computer system for violations of the Internet Usage Policy. Any violation of this policy will subject the employee to disciplinary action, possibly including termination.

2.4 Policy Exceptions

Employees are permitted to access the Internet for personal business during lunch and coffee breaks as long as the use is in strict compliance with the other terms of this policy. Exceptions for use of the Internet for school or other purposes are allowed with the approval of the division director.

Divisions of the Office of Management and Budget may adopt more restrictive policies at their discretion.

Appendix L: Secretary of State

Business Communication Systems Policy

Business communications includes telephone, facsimile (fax) machines, all computer software, and any other type of electronic communication.

The Secretary of State's computers and electronic communication systems are the property of the agency. Telephone, fax machines, and computer software, including electronic mail and Internet, are resources provided as business communication tools. These tools shall be used for matters directly related to the business activities of the Secretary of State and as a means to further the agency mission.

Employees are expected to communicate in a professional manner that will reflect positively on them and the Secretary of State. Vulgar, profane, insulting or offensive messages including racial or sexual slurs are unprofessional. Soliciting outside business ventures, advertising or soliciting for personal enterprises, and "chain letters" are prohibited. Limited, local use of business communications for personal purposes is permissible during breaks, lunches, and personal time outside normal business hours.

Employees that transmit, receive, or store private electronic communications do so at their own risk. Any transmissions sent or received through the agency's system are not considered private and may be monitored and reviewed as needed to ensure the proper use of the system and to protect the interests of the agency. System features such as passwords and delete message functions give the appearance of privacy, but do not affect the agency's ability to retrieve and right to review electronic messages.

Employees are not to use security features such as codes or passwords without the express knowledge and prior approval of their division director. No employee shall send E-mail under another employee's name without authorization. No employee shall alter and forward any portion of a received message which relates to the business activities of the Secretary of State.

All agency electronic mail is an official public record and is subject to public record regulations with respect to inspection, disclosure, scheduled retention, and disposition. E-mail records must be addressed on a records retention schedule when they meet the following criteria:

Made or received under state law or in the conduct of official agency business.

Preserve evidence of the agency's organization, functions or other activities.

Contain information relating to agency programs, policies, decision, and essential transactions.

As a condition of continued employment, all current employees are required to sign a Business Communication Acknowledgment <51554.pdf>. New employees are required to sign this form upon acceptance of employment.

A violation of this policy may subject the employee to disciplinary action.

ss: Al Jaeger
Secretary of State

BUSINESS COMMUNICATION ACKNOWLEDGMENT
SECRETARY OF STATE
SFN 51554 (11-08)

I understand that all telephone, fax machines and computer software and all information transmitted by, received from, or stored in these systems is the property of the Secretary of State.

I understand that these systems are not to be used for soliciting outside business ventures, advertising or soliciting for personal enterprises and that "chain letters" are prohibited.

I have no expectation of privacy in connection with the use of this equipment or with the transmission, receipt or storage of information in this equipment.

I will not use another person's password, access a file or retrieve any stored communication, unless authorized. I acknowledge and give consent to monitoring the use of this equipment at any time.

Employee's Name (Please Print)

Employee's Signature Date

Appendix M: Unified Judicial System

UNIFIED JUDICIAL SYSTEM

Policy 213 June 16, 1999

COMPUTER USAGE

Microcomputers and peripheral equipment acquired by the Unified Judicial System will only be used for:

1. Financial administration;
2. Case information systems.
3. Legal research;
4. Word processing;
5. Development of new or enhancement of existing programs;
6. Other professional activities related to the Unified Judicial System.

This policy does not prohibit the limited use of state-owned computer equipment for nongovernmental purposes if all the following requirements are met:

(a) The use does not interfere with the performance of the employee's public duties;
(b) The cost or value related to the use is nominal;
(c) The use does not create the appearance of impropriety;
(d) The use is not for a partisan political purposes; and
(e) The use is not for personal commercial purpose.

Only Unified Judicial System justices, judges, and judicial employees are authorized, after completing training, to use this hardware.

SOFTWARE AND DATA USAGE

The Unified Judicial System has acquired the right to use several proprietary software packages. A license agreement governs the use of the software. Copies of all software license agreements should be filed with the Office of State Court Administrator. People who use the proprietary software should be aware of the agreements between the vendor and the Unified Judicial System. Each person using proprietary software purchased by the unified judicial system is responsible for protecting against any violation of the software license agreements. Typically the agreement states the uses which are NOT permitted, such as:

- making copies of the user's manual
- making copies of the system diskettes, tapes or other media, unless specifically told to do so in the documentation
- making alterations to the software source code OR
- provide use of the software in a multiple CPU or user arrangement to users who are not individually licensed.

Violation of any part of these agreements may create legal and financial liabilities for the Unified Judicial System and the responsible individual(s).

The following conditions govern the use and care of microcomputer hardware and software assigned to the Unified Judicial System staff:

- The improper reproduction of proprietary software by any means is prohibited.
- The use of proprietary software which is not the property of the Unified Judicial System on any computing devices belonging to the Unified Judicial System is prohibited unless authorized to do so in writing by the director of technology.
- The safeguarding of hardware and software assigned is the responsibility of the individual.
- The staff assigned the proprietary software will abide by the contractual agreements between the vendor of the proprietary software and the Unified Judicial System.

Data and software which reside on the State's mainframe or agency's mini or microcomputer is the property of the Unified Judicial System or other government agency. Use, alteration or deletion by unauthorized personnel is prohibited. Therefore, Unified Judicial System personnel should not connect Unified Judicial System microcomputers to the State network without written approval from the director of technology.

Passwords and identifications used to access the mainframe are confidential and should not be written down and should not be shared unless it expedites the office operations. If the Unified Judicial System personnel have any question regarding these guidelines they should contact the Supreme Court's director of technology. Unified Judicial System personnel who violate any of these guidelines are subject to disciplinary actions including dismissal.

USE OF THE INTERNET AND REMOTE ACCESS

The Internet (World Wide Web) is a vast, global network linking computers at sites around the world and it is a vital source for researching and accessing information, communicating through electronic mail (E-mail), and using on-line services.

Remote Access is a process of connecting via a communication line to the statewide network, which allows connection to the Microsoft NT and Exchange server, AS/400 and the Internet from a remote location.

Employees are encouraged to become familiar with and use the Internet's and the Remote Access resources to enhance productivity. The state court administrator's office is responsible for controlling the use of the Internet and Remote Access in a reasonable manner to prevent or detect abuse and avoid legal exposure.

1. Employees of the State Judicial System may use the Internet and Remote Access for a purpose related to their employment or official position. An employee may use the Internet and the Remote Access for a non-governmental purpose provided the use:

    a. does not interfere with the performance of the employee's public duties;
    b. is of nominal cost or value;
    c. does not create the appearance of impropriety;
    d. is not for personal commercial purpose;
    e. is reasonable in time, duration, and frequency; and
    f. makes only minimal use of hardware and software resources.

2. Training. The State Judicial System will offer training for employees on using the Internet and Remote Access so the employees become more informed, knowledgeable, and productive. The training will teach employees how to use the Internet and Remote Access effectively and avoid unlawful use. Training may include software, books, and off-site and in-house training.

3. Remote Access. The supervisor's approval is needed in order for Remote Access. In the districts, the Presiding Judge's approval is needed for Remote Access. This may be done in cases where it is necessary to carry out the work of the office or to facilitate the efficient use of equipment or employees. Without the supervisor's approval, a non-exempt employee may not use the Remote Access to work in excess of the standard 40-hour week.

4. Standards of Conduct. An employee's use of the Internet and Remote Access is a privilege, not a right. An employee is solely responsible and shall be personally liable, legally, financially, or otherwise, for the employee's use of the Internet and Remote Access outside the scope of the employee's employment. An employee's use within the scope of employment shall be treated as other activities undertaken by the employee within the scope of employment. An employee's inappropriate conduct may lead to disciplinary action, including restricting the employee's access and use of the Internet or other appropriate action. An employee:

    a. must use the Internet in a professional and ethical manner;
    b. may not create or distribute immoral, obscene, threatening, defrauding, or violent text or images or transmit inappropriate or unlawful materials through the Internet;
    c. may not enter or send obscene or offensive material into or through the Internet;
    d. may not create, distribute, or knowingly use unauthorized copies of copyrighted material on the Internet;
    e. must use the Internet only to access files that are publicly available or to which the employee has authorized access;

f. must refrain from overloading the network with excessive data or wasting computer time, connect time, disc space, printer paper, or other resources;
g. is responsible for any charges associated with billable Internet services unless appropriate authorization has been obtained prior to accruing the charge;
h. may not use illegal copies of copyrighted software, store such copies on the State Judicial System computers, or transmit them over the state networks or the Internet;
i. may be aware that all E-mail communications maybe subject to disclosure. An employee must not use E-mail:

    1) to harass, intimidate or annoy another person;
    2) to send foul, inappropriate, or offensive messages;
    3) to solicit outside business ventures; or
    4) to send messages that may be interpreted as sexual harassment.

The Judiciary may install software to measure and manage Internet and Remote Access usage. No person may intercept confidential communication except as provided by law.

Approved by the Supreme Court 06/16/99